Cellular Cryptography and GSM

igital cellular systems are on a growth curve to overtake analog systems in just a few years. More than five and a half million digital handsets were sold in 1997, up from less than one and a half million in 1996.

One of three digital technologies competing for customers in the United States is the Global System for Mobiles (GSM) standard. Originating in Europe in the early 1980s, GSM is now serving more than 100 million customers around the world, and more than two million subscribers in the United States.

Rather than holding customer information in the phone itself, each GSM telephone uses a removable, personalized smartcard called a Subscriber Identity Module (SIM). The SIM is actually a tiny computer, complete with memory storage and a low power microprocessor. Besides holding subscriber information, it also performs security functions to protect the customer and the network.

Probably the two most common areas of vulnerability in a cellular telephone network are fraudulent use of service and interception of call contents. The GSM SIM makes use of cryptography to reduce fraud and provide some measure of confidentiality.

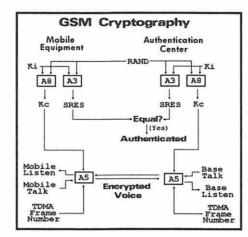
Before a SIM is released to a customer it is programmed with a unique, secret 128-bit long key called Ki. Once programmed, Ki is supposed to remain hidden and invisible, available only to special computer algorithms that run internally on the SIM. A copy of this secret key is also kept by the network operator in an Authentication Center (AuC).

The SIM also contains two cryptographic algorithms referred to as A3 and A8, which are used for authentication and confidentiality.

Authentication

One of the primary security functions of the SIM is to *authenticate* the subscriber to the network. A GSM network verifies the identity of a subscriber through a *challenge-response* process. When a mobile subscriber requests service, the network sends a mathematical challenge to the phone, which it must answer correctly before being granted access.

The challenge sent by the network to the phone consists of a 128-bit number called RAND. When the phone receives the RAND challenge it passes it into the SIM for process-



ing. The SIM card sends RAND and the secret 128-bit key Ki through the A3 algorithm to produce a 32-bit "signed response" (SRES). This number is transferred out of the SIM into the phone, where it is then transmitted to the network. This is the phone's response to the network's challenge.

Meanwhile the network has performed the same set of operations. Using the same value of RAND and an identical copy of Ki, the network has computed its own value for SRES.

The network compares the SRES received from the phone to its own SRES: If the two values are the same, it assumes the phone is legitimate and allows service to proceed. If the two values are not the same, the network assumes the SIM does not have the proper secret key Ki and therefore denies service to the phone.

Since the RAND value changes with every access attempt, an eavesdropper recording the SRES response will not be able to successfully reuse it later. Even if by chance a particular RAND challenge happened to be reused, a GSM network has the flexibility to authenticate the phone as often as it wishes, perhaps several times throughout the duration of a call. A legitimate phone can easily return the correct answer each time, whereas a cloned phone using a single successful SRES will be thwarted.

Confidentiality

The SIM also provides information needed to encrypt the radio connection between the phone and the base station. In order to understand how the encryption works, a little background is necessary.

GSM uses a technique called time division to share the radio channel with up to seven other users. Each user takes turns using the common radio channel, sending and receiving information only during one of the eight available time slots. Each time slot is very short, lasting only about 4.6 milliseconds, and is identified by a frame number. A GSM conversation uses two frames, one going from the base station to the phone (called the forward direction) and another going from the phone back to the base station (called the reverse direction). Each of these frames contains 114 bits of user information, which is almost always digitized and compressed speech.

So, every 4.6 milliseconds the phone receives 114 bits of information from the base station and transmits another 114 bits to the base station. It is these 228 bits that require encryption to protect them from eavesdroppers.

Using the RAND challenge and the secret key Ki, the SIM runs the A8 algorithm to produce a 64-bit long cipher key called Kc. Kc is transferred out of the SIM and into the phone, where it is used by a third algorithm called A5.

A5 uses Kc and the current frame number to produce a key stream of 228 bits, half of which decode the incoming forward channel and the other half encode the outgoing reverse channel. A5 resides in hardware in the phone, not in the SIM, and must operate quickly and continuously to generate a fresh set of 228 bits every 4.6 milliseconds. Also, because GSM handsets are designed to operate in different networks, the A5 algorithm must be common to all GSM networks.

There are presently at least two different implementations of A5. The first, called A5/1, provides the strongest level of encryption across the air link. Although purportedly using 64 bit keys, in actual practice the keys are no more than 54 bits long. The second, A5/2, uses a 16-bit key and is designed for export to non-Western countries.

Since encryption requires additional hardware in each base station, raising the cost and complexity of the network, a third option is to employ what's euphemistically called A5/0—that is, no encryption at all.

Weaknesses

GSM security is based on keeping Ki a secret. If Ki could somehow be extracted from a SIM, the holder would be able to create a duplicate SIM. As demonstrated in April of this year, there is a weakness in most GSM networks that allows Ki to be determined.

The A3 and A8 algorithms are really interface specifications, not the actual routines themselves. A3 and A8 define the inputs (RAND and Ki) and the outputs (SRES and Kc) of each algorithm, but don't specify exactly how each will produce their result. Each GSM network operator can basically implement whatever security routines they wish as long as the inputs and outputs match the definitions for A3 and A8. In addition, since A3 and A8 take the same inputs, a combined algorithm called A38 is also defined.

GSM specifications provide a "reference implementation" for A38, spelling out the details of an example computer program that will produce SRES and Kc. It turns out that almost all network operators have implemented this example, referred to as COMP128.

COMP128 was designed in secret and released only to a limited number of groups under strict non-disclosure agreements. Its strength was based on what cryptographers call *security through obscurity*, relying on that fact that since so few people knew the details no one would find any weaknesses and the algorithm would remain unbroken.

As usually happens with this type of "security," the details of COMP128 were eventually pieced together from leaked documents and other data. A group of researchers in California assembled the algorithm and soon found that it had a serious flaw.

COMP128 is what's known as a *hash* function. To generate an answer to a network challenge it takes a total of 256 bits of information (RAND and Ki) and produces a 32-bit answer (SRES). Because there are so many possible values of RAND as compared to possible SRES values, it is likely that more than one value of RAND will produce the same SRES. This is known as a *collision*, and in the case of COMP128 it turns out that such collisions "leak" information about Ki.

By selecting the proper values of RAND, an attacker can eventually determine the value of Ki by examining the SRES collisions. Using a smart card reader and some custom software, in April of this year the researchers demonstrated this attack by extracting the secret key from a Pacific Bell SIM in about eight hours. Their software repeatedly requested that the SIM execute the COMP128 authentication algorithm and examined the

results, slowly piecing together the value of Ki. Once they had the secret key they copied it into another SIM card and effectively cloned a GSM phone.

The researchers also discovered an interesting fact about Kc, the cipher key used to encrypt the contents of a GSM call. Although Kc is a 64-bit key, the COMP128 algorithm forces the last 10 bits to all zeros, effectively reducing it to a 54-bit key. It appears that the original designers, probably under pressure from intelligence and law enforcement agencies, deliberately weakened the protection that A5 provides.

The law in the United States requires a court order before a law enforcement agency is allowed to wiretap a telephone, cellular or otherwise. Legal wiretaps are almost invariably performed at the mobile switching center, where the mobile network joins with the rest of the public telephone network. The call at that point is carried over wires that can easily be tapped, making eavesdropping relatively easy. Very few legal wiretaps are done by intercepting the radio portion of the call, since it's much easier, safer, and more reliable to do so at the switch. Why then would law enforcement agencies be interested in weak radio encryption, if not to perform illegal wiretaps?

■ Wireless Surveillance

Things are still boiling on the legislative

front regarding wiretapping. If you recall, in 1994 Congress passed the Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications equipment and service providers to make the nation's wired and wireless telephones "wiretap friendly." Providers and equipment manufacturers are facing an October deadline to meet a set of compliance requirements that haven't yet been approved by all sides.

The telecommunications industry, as required by CALEA, has developed a set of technical standards to implement the law. The FBI, representing the nation's law enforcement agencies, has blocked implementation of the standards, arguing that they don't go far enough in providing surveillance capabilities. The FBI has a "punch list" of requirements that the telecommunications industry and privacy advocates say goes far beyond what Congress intended and what CALEA allows.

This spring the deadlock ended up in the hands of the Federal Communications Commission (FCC), who will study the issue, take public comments, and eventually issue a ruling to arbitrate the dispute.

More information on GSM, CALEA, and other wireless topics is available on my website at www.decode.com, and in my book *Inside Mobile Telephone Systems* from Index Publishing. I am also reachable via electronic mail at dan@decode.com. Until next time, happy monitoring!

